CLEAN VERSION OF SPECIFICATION PARAGRAPHS

LOCALLY ADAPTABLE CENTRAL SECURITY MANAGEMENT IN A HETEROGENEOUS NETWORK ENVIRONMENT
Applicant: Daniel Jay Thomsen et al.
Serial No.: 09/483,164

SMC 8/28/07 **Please insert the following paragraph at page 1, line 5:**

Statement Regarding Government Rights

This invention was made with Government support under Contract F30602-97-C-0245 awarded by the Air Force. The Government has certain rights in this invention.

IN THE SPECIFICATION

Please amend the specification as follows:

The paragraph beginning at page 6, line 12 is amended as follows:

System 10 uses [[an]] a layered approach to Role-Based Access Control (RBAC). In one embodiment, as is shown in Fig. 2, security management system 10 includes a multi-layered RBAC model 20 for unifying diverse access control mechanisms into a single environment, a Graphical User Interface (GUI) 22 for manipulating model 20, and translation software 24 for translating a security policy defined by GUI 22 to specific access control mechanisms 26.1 through 26.N.

The paragraph beginning at page 11, line 10 is amended as follows:

In one embodiment, the building blocks of system 10 are called keys. A key represents the ability to access some resource[,]; just like in the real world where having a key allows a person to open a door. Keys become an atomic unit of the security policy. A key cannot be divided into smaller access control pieces. As shown in Fig. 7, application keys 40 formed at the application developer layer are passed up to semantic layers 36 and combined and passed to the next layer. The process continues up ~~top~~ to layer 32, which binds users to the policy pieces.

The paragraph beginning at page 24, line 14 is amended as follows:

While the hospital is tied to a regional information ~~net work~~ network, it employs a small staff that must wear many hats. The system administrator uses system 10 to create three key chains to assign to users: the DOCTOR key chain 74 contains only the PROVIDER key 76, the INSURANCE key chain 78 contains only the REVIEWER key 80, and the CLERK key chain 82 contains only the ADMIN key 84.

The paragraph beginning at page 25, line 12 is amended as follows:

A "work product" is an artifact created or modified by steps. Steps use and produce work products. A "role" represents the accesses that are required to ~~per form~~ perform a step. A "workflow condition" is a predicate that must be satisfied during step performance. It is often expressed as entry and exit conditions on the step, that is, the step can begin when and can end

when the conditions are true. A "performer" is a person or tool with the skills necessary to complete the step. A role may require special skills and therefore a specific performer. Finally, a "method" is an approach for carrying out a step. A step can be performed using one of several methods. The performer can do these methods.

B4

SMC 8/28/07 **The paragraph beginning at page 28, line 30 is amended as follows:**

Our initial investigation focused on ways to enforce work flow entirely within the local enforcement mechanisms. To satisfy workflow's central enforcement needs, it was thought that a workflow object would track the current step for each instance of a workflow. That is, system 10 would create the workflow object and bind it to the resources it controls. For each access request, the local enforcement mechanism would ~~ex amine~~ examine the corresponding workflow object and verify that the request is approved for the current step. If the request is approved, the local policy ("pushed out" as usual by system 10) would be enforced for that resource. The local enforcement mechanism would update the workflow object's indicator of current step as required.

B5

SMC 8/28/07 **The paragraph beginning at page 29, line 20 is amended as follows:**

Policy enforcement can be partitioned into three layers, from lowest to highest: controlling access to resources, controlling access to steps and application-specific enforcement. A useful split occurs in the middle, or step, layer. Steps are a natural primitive for workflow designers. A WMS is specialized to create steps, determine their proper order and control execution of work flow instances according to that order. These operations are unique to workflow technology. However, access for a particular role to the resources associated with a particular step can be controlled by mechanisms that are commonly available in ~~non-workflow~~ non-workflow domains.

B6

The paragraph beginning at page 32, line 10 is amended as follows:

In addition, system 10 provides a method for adding [[an]] and removing applications with minimal impact on other semantic layers, or on the local system administration layer. In a

B7

B7 manner similar to the OSI TCP/IP model, clearly defined semantic boundaries can be used to create plug-and-play system security.

SMC 8/28/07 **The paragraph beginning at page 18, line 12 is amended as follows:**

The third difficulty arises from the fact that low level constraints 44 could be modified in a single place and that these changes would directly impact all the senior roles. Consider the policy in ~~Figs. 11a and b.~~ Figs.13a and b. In Fig. 13a, system 10 includes role inheritance. In such an approach, the local policy has changed; now, all employees were allowed to browse the web. With a role hierarchy the "browse" key could be added to the employee node and the permission would automatically flow up the hierarchy.

B8